REMARKS

Dependent claims 9-11 were found to be allowable if rewritten in independent form including all the limitations of the base claim and any intervening claims. This has been done above, so these claims should be allowed.

Independent claim 21 and its dependents 22-24 were found to be allowable.

Claims 1, 3-4, 6-7, 12, 25 and 28 were rejected under 35 USC 103(b) based on US Patent 5,991,881 to Conklin et al. and US Patent Publication 2003/0212821 by Gillies et al.

Claim 1 recites in part, "fifth program instructions, responsive to the packet not being a known exploit, AND the packet not being addressed to a broadcast IP address of a network AND the packet not being network administration traffic AND the packet not being another type of traffic known to be benign, to determine and report that the packet is a new, exploit candidate".

Conklin et al. discloses the following Attack Checks: pattern matching including checking for strings of data within packets, and artificial intelligence including comparing incoming packets against historical data captured over time. See Figure 7 and Column 7 lines 50-55. Conklin et al. also discloses in Figure 7 that a series of Attack Checks are performed, but does state anything additional as to the nature of these Attach Checks. Conklin et al. also discloses that if any Attach Check/test indicates an intrusion that additional information about the attack is collected:

> "As the Attack Checks are comparative, techniques as used in the preferred embodiment include pattern matching, such as checking restraints and vehicle within packets and the use of artificial intelligence for comparing incoming packets against historical data captured over time. **If an Attack Check indicates an intrusion, then an Attack Identifier is prepared providing information regarding the time of day, packet type, the attack type, and the source or destination address of the attack** and sent to an attack handler shown in the

preferred embodiment as the Evidence Logging—Event Log Analyzer Process as shown in FIG. 8." (emphasis added) Conklin Column 7 lines 50-60.

However, Conklin et al. does not disclose the series of ANDed tests recited in claim 1 to determine whether a potential attack has occurred, i.e. "fifth program instructions, responsive to the packet not being a known exploit, AND the packet not being addressed to a broadcast IP address of a network AND the packet not being network administration traffic AND the packet not being another type of traffic known to be benign, to determine and report that the packet is a new, exploit candidate". As indicated by the types of Attack Checks stated in Conklin et al. as noted above, Conklin et al. does not consider whether the packet is addressed to a broadcast IP address of a network or the packet is network administration traffic. Therefore, Conklin et al. does not teach or suggest key features of claim 1, and therefore, does not form a prima facie case of obviousness.

The Examiner acknowledges that Conklin et al. "does not disclose the packet addressed to a broadcast address", but cites Gillies et al. as purportedly filling this gap. Gillies et al. teaches a technique for routing packets in a network, and pertains to the routing technique, not intrusion detection.

"[0023] Described herein are systems and methods for routing communication packets over wireless and wired networks. Routing may be implemented at either the MAC layer or the Internet layer. Communication packets that are routed include both application data and objects containing network optimization parameters that are used to control the physical links (e.g., radio) in the network. This routing protocol is partitioned into two pieces, a data-transport sub-layer and an open object definition sub-layer. The routing system includes a triggered unreliable update mechanism, and a periodic reliable update mechanism to propagate routing information throughout the network and recover from packets lost in the network. The system provides a clean separation between the routing transport protocol and the objects to be routed. Advantageously, new types of objects can be defined and propagated throughout the routing system, including information that has no relationship to network topology or link performance parameters." Gillies et al.

Gillies et al. also teaches a "forwarding system" which determines whether to retransmit a packet if its final destination is elsewhere, or process it if its final destination has been reached:

> [0052] FIG. 2A is a block diagram illustrating an example routing device **40** according to an embodiment of the present invention. In the illustrated embodiment, the routing device **40** comprises a forwarding system **60**, an attribute management system **70**, a network interface **80**, and a data storage area **90**. As previously described, the routing device **40** can be any device with the ability to communicate over a wired or wireless network.
>
> [0053] The forwarding system **60** is preferably a hardware or software module integrated with the MAC layer of the communication protocol on the routing device **40**. Alternatively, the forwarding system **60** may be integrated with the Internet layer of the communication protocol. **The forwarding system** 60 **preferably examines communication packets received from the network and processes those packets or retransmits those packets (or both) as necessary. For example, the forwarding system** 60 **may receive a communication packet from the network and determine that the packet is destined for another network device.** Accordingly, the forwarding system **60** may retransmit the communication packet or discard the packet, depending upon the final destination of the packet." (emphasis added) Gillies et al.

However, Gillies et al. does not consider whether the packet is addressed to a broadcast IP address of a network or the packet is network administration traffic as factors in determining whether the message is a potential intrusion, as recited in claim 1. Gillies et al. merely checks the destination address of the packet to determine if the packet should be transmitted further or processed and discarded after processing. Therefore, Conklin et al. in combination with Gillies et al. do not form a prima facie case of obviousness.

During a telephonic interview with Examiner Perungavoor on September 1, 2011, **the Examiner withdrew the rejection of claims 1 and 25 and their dependents based on Conklin et al. and Gillies et al.** because the repetition of "attack checks" in Figure 7 does not teach the consideration of whether the packet is addressed to a broadcast IP address of a network or the packet is network administration traffic as recited in claims 1 and 25. Rather, these "attack check" steps can be repetitions of the pattern matching or historical comparisons explained in Figure 7 and Column 7 lines 50-55, or something else which is unspecified. The Examiner stated that he would conduct another search of claims 1 and 25 in the context of intrusion detection. Until such time as the Examiner finds prior art to support a 35 USC 102 or 35 USC 103 rejection, Applicants maintain the allowability of claims 1 and 25 and their dependents.

Claims 3-4, 6-7 and 12 depend on claim 1, and therefore, should be allowable for the same reasons as claim 1.

Independent claim 25 distinguishes over Conklin et al. and Gillies et al. for the same reasons that claim 1 distinguishes thereover.

Claims 26-28 depend on claim 25, and therefore, distinguish over Conklin et al. and Gillies et al. for the same reasons that claim 1 distinguishes thereover.

Based on the foregoing, Applicants request allowance of the present patent application as amended above.

Respectfully submitted,

Dated: 9/2/2011
Telephone: 607-429-4368
Fax No.: 607-429-4119

/Arthur J. Samodovitz/
Arthur J. Samodovitz
Reg. No. 31,297